MATH/CS 295: CRYPTOGRAPHY
HOMEWORK #7 ADDITIONAL PROBLEMS

Problem 2.B. Let G be a group with $\#G = n$ and let $g \in G$.

(a) Show that if $h \in G$ and $hg \neq gh$ then $\log_g h$ is not defined.

(b) Show that $G = \langle g \rangle$ if and only if $g^{n/\ell} \neq 1$ for every prime $\ell \mid n$.

(c) Conclude that $g \in (\mathbb{Z}/p\mathbb{Z})^*$ is a primitive root if and only if $g^{(p-1)/\ell} \not\equiv 1 \pmod{p}$ for every prime $\ell \mid (p-1)$, and hence given the factorization of $p-1$ one can determine if g is a primitive root efficiently. Use this to verify that 3 is a primitive root modulo 65537.